Long Term Cybersecurity research
Summaries of projects granted in the first NWO call for proposals (2012)

Project number	CYBSEC.12.015 / 628.001.007	
Main Applicant	Dr. L. Batina	Radboud Universiteit Nijmegen Faculteit der Natuurwetenschappen, Wiskunde en Informatica Institute for Computing and Information Science
Project title	Profiling for Optical Fault Induction using Location-dependent leakage (ProFil)	

Scientific summary

We increasingly rely on embedded security systems in our lives, such as smart cards and RFID tags that are used for public transport, access control, and pay-TV systems. Ensuring the security and privacy requirements of these systems is a challenging problem, as witnessed by the breaking of the cryptosystems used in mobile phones, car keys, and RIFD-enabled cards (the Dutch "OV-chipkaart''). This proposal focuses on physical attacks, the main threat to the security of next generation smart devices. In such attacks information about some physical (also called side-channel) leakages e.g. power consumption data is collected and analyzed allowing an adversary to retrieve secret keys of the device.
Fault injection is another, more active type of side-channels as it relies on the process of introducing temporary computation errors in a chip. With this attack, also the location on the chip where the faults are induced is very important as automated searches are not possible. Recently, new results showed the benefits of exploring locally-based electromagnetic leakages and photonics emissions finding in this way sensitive areas where the keys are manipulated.

The main idea of this project is to introduce a profiling phase for fault injection using other passive side-channels. To this aim, we will use high-resolution EMA and optical emissions. We will develop theoretical framework for fault analysis that will be verified using state of the art equipment and tools. The participation of Riscure will provide a suitable industrial environment to test and apply the algorithms and countermeasures developed during the project.

Applicable NCSRA theme

- Secure design & engineering